Graham B. LippSmith (SBN 221984)
g@lippsmith.com
MaryBeth LippSmith (SBN 223573)
mb@lippsmith.com
Jaclyn L. Anderson (SBN 258609)
jla@lippsmith.com
LIPPSMITH LLP
555 S. Flower Street, Suite 4400
Los Angeles, California 90071
Tel: (213) 344-1820 / Fax: (213) 513-2495

Jeremy M. Glapion
Admitted Pro Hac Vice
jmg@glapionlaw.com
GLAPION LAW FIRM
1704 Maxwell Drive
Wall, New Jersey 07719
Tel: (732) 455-9737 / Fax: (732) 965-8006

Jason T. Dennett (WSBA #30686)
Admitted Pro Hac Vice
jdennett@tousley.com
Kaleigh N. Boyd (WSBA #52684)
Admitted Pro Hac Vice
kboyd@tousley.com
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
Tel: (206) 682-5600 / Fax: (206) 682-2992

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MICHAEL MCGINNIS and CYNDY BOULTON, individually, and on behalf of all others similarly situated; Plaintiffs, v. COMMUNITY.COM, INC.; Defendant.	Civil Case No.: 2:23-cv-02426-SB-JPR **PLAINTIFF'S OPPOSITION TO DEFENDANT COMMUNITY.COM, INC.'S MOTION TO DISMISS** Date: August 18, 2023 Time: 8:30 a.m. Court: Courtroom 6C Judge: Hon. Stanley Blumenfeld, Jr. Date Action Filed: March 31, 2023 Trial Date: August 5, 2024

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

INTRODUCTION

This Court is already familiar with the background of this case. *See Adler v. Community.com, Inc.*, Case No. 2:21-cv-02416-SB-JPR, 2021 WL 4805435 (C.D. Cal. Aug. 2, 2021). Defendant Community.com, Inc. ("Defendant" or "Community") operates a honeypot. It uses celebrities—including social media influencers, television stars, and professional athletes—to lure unwitting consumers, through social media and other means, to contact those celebrities on specific telephone numbers. Those celebrities hold out those telephone numbers as their personal and direct numbers and even take steps to preempt any doubt that the numbers are actually theirs. Likely thousands of people, ranging from minors to the elderly, and including Plaintiff Cyndi Boulton ("Plaintiff"), have responded to these invitations, excited to talk directly with a celebrity they may idolize (or despise).

What Defendant does not disclose is that it will intercept, log, and read consumers' initial messages to these celebrities, and that it will hold those messages hostage from the intended celebrity unless and until the sender signs up for Defendant's social networking site. In fact, in the intervening time since the *Adler* case was voluntarily dismissed, Defendant has doubled down on its eavesdropping and gatekeeping role. Its privacy policy now claims the right to "access, review, block (including limiting Community Leaders' ability to access messages), or delete your messages at any time and for any reason."

///

Yet Defendant's involvement and policies are not revealed until after the first message is sent. This is by design. Defendant's entire business model is predicated on giving the appearance of texting celebrities the same way you might with anyone else. This illusion—and it is nothing more—would be shattered if Defendant disclosed that it intercepts, logs, reads, and withholds the messages consumers send to its celebrity clients for its own ends.

Defendant's conduct violates two separate provisions of the California Invasion of Privacy Act ("CIPA").[1]

BACKGROUND

On April 7, 2022, LL Cool J posted a video on TikTok. Complaint ("Compl.") ¶ 45. He told his followers, "I've come up with this crazy idea for us to stay connected. I'ma give you my phone number. I know it's crazy." *Id.*

When someone attempts to text LL Cool J's "number," however, the message does not go to LL Cool J. *Id.* ¶¶ 48–49, 53. Instead, any initial text is redirected to Defendant. Defendant then holds the message hostage, sending two automated texts requiring the sender to sign up for Defendant's social networking site in order to reach LL Cool J. *Id.* ¶ 53.

This bait-and-switch is Defendant's business model. *Id.* ¶ 23. Defendant's celebrity and influencer clients ("Community Leaders") number more than 900 at last

[1] Plaintiff preserved arguments under CIPA § 631 and the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1)(a). Dkt. 36.

count and include LL Cool J. *Id.* ¶¶ 24, 56. These Community Leaders receive an assigned telephone number, which they then present as "their" number at which fans and others can communicate directly with them. *Id.* ¶¶ 16–17. Defendant also works with its Community Leaders to come up with scripts or general ideas on how to best discuss "their" number to the public. *Id.* ¶ 57. And the Community Leaders themselves, again in conjunction with Defendant, take steps to preempt any doubts that the number is actually theirs, no matter how "crazy" it may sound. *Id.* ¶ 61. Only after someone texts the number do they learn that the number is not actually the Community Leader's personal, direct phone number, but is, instead, part of a social media service for which the person must sign up before being able to ostensibly text with the celebrity. *Id.* ¶¶ 20–21. The more people who sign up for Defendant's celebrity-specific "group" within Defendant's social media site, the more Defendant charges that Community Leader for building their brand. *Id.* ¶ 22.

Most troubling, Defendant, per its own privacy policy, "collect[s] . . . the contents of the text message" and "whether the message includes a particular word, phrase, or emoji." *Id.* ¶ 29. Defendant claims the right to "analyze your … Messaging Info" to generate insights about the sender and to operate its platform. *Id.* ¶ 32. Defendant also claims the right to access, review, and arbitrarily withhold messages from reaching their intended Community Leader. *Id.* ¶ 33. While this language might (legally) protect Defendant's interception, recording, and reading of text messages sent *after* a person signs up for Defendant's services and agrees to its terms and

privacy policy, consumers never see this disclosure before sending their initial text. *Id.* ¶ 34. Plaintiff Boulton sent a text message to the number that LL Cool J announced was "[his] phone number." *Id.* ¶ 46. When she sent the text, she did not consent to—and was not even aware of—Defendant's interception, hijacking, recording, and reading of the message she intended for LL Cool J. *Id.* ¶¶ 54, 58, 66, 67.

Accordingly, Plaintiff filed this case, alleging Defendant violated three separate provisions of CIPA and the Electronic Communications Privacy Act ("ECPA"). Plaintiff has stipulated to the dismissal of the CIPA claim under Section 631 and the ECPA claim while preserving all rights related thereto. *See* Dkt. 36.

LEGAL STANDARD

Under Rule 8(a), Plaintiff need only set forth enough facts to state a plausible entitlement to relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). Thus, on a motion to dismiss, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). "In deciding whether the plaintiff has stated a claim upon which relief can be granted, the Court accepts the plaintiff's allegations as true and draws all reasonable inferences in favor of the plaintiff." *Anderson v. Apple Inc.*, 500 F. Supp. 3d 993, 1004 (N.D. Cal. 2020) (citing *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987)).

///

DISCUSSION

I. Plaintiff Boulton Has Standing to Pursue Her Claims

Plaintiff Cyndi Boulton "suffered an injury in fact." "[T]o establish standing, a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, __ U.S. __,141 S. Ct. 2190, 2203 (2021).

"Courts must afford due respect to Congress's decision to impose a statutory prohibition or obligation on a defendant, and to grant a plaintiff a cause of action to sue over the defendant's violation of that statutory prohibition or obligation." *Id.* at 2204. In so doing, Congress elevates previously inadequate injuries to the status of "concrete, *de facto* injuries." *Id.* (citation omitted). Notwithstanding a statutory cause of action, courts must still examine whether there exists a concrete harm to the plaintiff. *Id.* at 2205.

Privacy right violations, as alleged here, are sufficiently concrete injuries-in-fact to confer Article III standing, independent of any statutory obligation. In *Wakefield v. ViSalus, Inc.*, the Ninth Circuit explained that *TransUnion*, "strengthens the principle that an intangible injury is sufficiently 'concrete' when (1) Congress created a statutory cause of action for the injury, and (2) the injury has a close historical or common-law analog." 51 F.4th 1109, 1118 (9th Cir. 2022). As the court in *Garcia v. Build.com* explains, case law holds that a CIPA violation

is a privacy violation, which is a concrete harm. No. 22-cv-01985-DMS-KSC, 2023 WL 4535531, at *4 (C.D. Cal. July 13, 2023). The *Garcia* court further explains that such case law is not undermined by the holding in *TransUnion* because *TransUnion* was a reiteration of the Supreme Court's decision in *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016), which predates that case law. *Id.* at *3.

The *Garcia* court ruled that "a CIPA violation is a violation of privacy rights and is a sufficiently concrete injury-in-fact" to establish Article III standing. *Id.* The court then concluded that the plaintiff's allegation of the defendant having "secretly intercepted and recorded Plaintiff's chat messages without informing her and without her consent" was "a sufficiently concrete and particularized injury" to confer Article III standing. *Id.* The *Garcia* court arrived at this conclusion while still acknowledging that other courts have found no standing where no personal information was disclosed, including this Court's holding in *Byars v. Sterling Jewelers, Inc.*, No. 5:22-cv-01456-SB-SP, 2023 WL 2996686 (C.D. Cal. Apr. 5, 2023). *See id.*

In *Byars*, the plaintiff was "a self-described 'tester' who visits websites 'to ensure that companies . . . abide by the strict privacy obligations imposed upon them by California law.'" *Byars*, 2023 WL 2996686, at *2. This Court considered the undisputed evidence that the plaintiff may not have used the chat function at issue at all (*id.* at *3–*4) and that the plaintiff fully expected her chats to be recorded (*id.* at *5–*6). There is no such evidence in this case. This Court also

specifically noted the difference between the facts in *Byars* and those in *Osgood v. Main Street Mktg, LLC*, No. 16-cv-2415-GPC, 2017 WL 131829 (S.D. Cal. Jan. 13, 2017), where "the plaintiffs alleged that they reasonably expected that their telephone calls were not being recorded." *Id.* at *5–*6. Plaintiff Boulton reasonably expected that her text communication would not be eavesdropped upon or received and recorded by Defendant. Compl. ¶ 59. Finally, Plaintiff did not and could not consent to Defendant's interception, eavesdropping upon, or receipt and recording of her text communication since she was not aware of Defendant's involvement or its practices (*id.* ¶ 54), while the *Byars* plaintiff arguably consented to the recording of her chats because she expected that recording.

Just as in *Garcia*, the formulation in *Wakefield* confirms that Plaintiff has standing. First, the California legislature created a cause of action in the CIPA statute, under which Plaintiff asserts claims here. Plaintiff also asserts claims under the ECPA, which was similarly enacted "to afford privacy protection to electronic communications." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2001). Second, "the Ninth Circuit concluded in *Wakefield* that traditional claims for invasion of privacy, intrusion upon seclusion, and nuisance are evidence of a common law analog to privacy violations." *Garcia*, 2023 WL 4535531, at *4 (internal quotation marks and citation omitted). Thus, Plaintiff asserts statutory causes of action and claims the concrete injury of an invasion of her privacy, providing the common law or traditional analog necessary to confer standing for

these statutory violations.

Plaintiff further alleges that "[t]he promotion of celebrities' purported phone numbers gives consumers an objectively reasonable expectation of confidentiality and that an interloper is not overhearing or recording the conversation." Compl. ¶ 59. This is especially true because Community Leaders use language "which suggests personal conversation." *Id.* ¶ 66. Thus, Plaintiff expected her text message to go only to LL Cool J. Instead, Community prevented that message from ever getting to LL Cool J. When anyone "first sends a text to a celebrity, at a number held out by that celebrity as their direct number, Defendant *prevents* that message from reaching that celebrity, records and scans its contents, and only allows it to continue its journey to the celebrity if the consumer signs up for Defendant's site *and* Defendant deems the message content acceptable." *Id.* ¶ 38. Further, Plaintiff alleges actual eavesdropping (*id.* at ¶ 73), and actual interception and recording of the communications intended for LL Cool J (*id.* at ¶¶ 46, 108–11, 116–19, 123–26, 130, 132–34).

TransUnion is, thus, distinguishable. *TransUnion* is a defamation case, and "[p]ublication is essential to liability in a suit for defamation." 141 S. Ct. at 2209. In *TransUnion*, the defendant's use of a particular system resulted in thousands of consumers being labeled "as potential terrorists, drug traffickers, or serious criminals" in credit reports issued by TransUnion. *Id.* But the defendant never disseminated the erroneous credit reports of more than 6,000 class members. *Id.* at

2200, 2209. There, the plaintiff argued that those class members had standing because of the "material risk that the information would be disseminated in the future." *Id.* at 2210. In contrast, Plaintiff Boulton is making claims for a past, tangible harm: invasion of privacy by the eavesdropping on and blocking of a communication intended for LL Cool J. The acts of eavesdropping and interception on a private communication are the claimed privacy violations, and no next step such as dissemination is required to establish those violations.

In addition, Plaintiff is not "merely seeking to ensure a defendant's compliance with regulatory law (and, of course, to obtain some money via the statutory damages)." *Id.* at 2206 (internal quotation marks and citation omitted). Plaintiff had a private communication surreptitiously intercepted, accessed, and withheld without her prior consent, and that is a violation of her right to privacy in her electronic communications.

Finally, Plaintiff can allege the concrete harm of distress if granted leave to amend. In *TransUnion*, the Supreme Court noted that there was no evidence of other injury "such as an emotional injury" to the class members who did not have their credit reports disseminated to a third party. 141 S. Ct. at 2211. In considering allegations on behalf of class members who received incorrectly-formatted credit report notices from the defendant, the Court similarly noted that there was no evidence that those notices caused those class members harm such as being "confused, distressed, or [having] relied on the information in any way." *Id.* at

2213–14 (internal quotation marks and citation omitted). Here, Plaintiff can—if granted leave—amend her allegations to include statements that she was distressed and disappointed when she learned that Defendant intercepted her text communication intended for LL Cool J and that her message never made it to him.

II. Defendant Violated CIPA Section 632

Section 632 provides for liability when "[a] person . . . intentionally and without the consent of all parties to a confidential communication . . . uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties or by means of a telegraph, telephone, or other device." Cal. Penal Code § 632; *Smith v. LoanMe, Inc.*, 11 Cal.5th 183, 190 (2021).

Distilled, Plaintiff must plead that Defendant (1) used an electronic amplifying or recording device (2) to eavesdrop upon or record (3) a "confidential communication" (4) without the consent of all parties to the communication. *See Wilborn v. Greystar Real Estate Partners, LLC*, 2013 WL 12111764, *2 (S.D. Cal. Jan. 8, 2013).

Defendant takes issue with the first and third of these elements. It argues that its software application cannot qualify as an "electronic amplifying or recording device" and that its text messages cannot qualify as "confidential communications." Neither argument is correct.

///

A. Defendant's application should qualify as a "device."

Section 632 does not define "electronic amplifying or recording device," and there is limited case law in the CIPA context discussing whether software or code can qualify. The only courts known to address this issue in the CIPA context assumed, without deciding, that software or code can qualify as devices for the purposes of the statute. *See Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, *3 (N.D. Cal. Oct. 23, 2019) (interpreting the phrase "device which is primarily or exclusively designed or intended for eavesdropping" under Section 635 and writing, "At the pleading stage, the Court must assume the truth of [Plaintiff's] allegation that [Defendant's] code is a device . . . ."); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 523 (C.D. Cal. 2021) ("The court need not address the parties' arguments as to whether FullStory's software constitutes a 'device' under CIPA . . . ..").

Seizing on this ostensible ambiguity, Defendant contends that its "software application" cannot be a "device" because it is not tangible.[2] Defendant's Motion to Dismiss ("Mot."), Dkt. 32, at 10–11. Defendant does not cite a single Section 632 case for its position, and its cited definitions do not limit "device" to something "tangible." *See, e.g.*, *Moreno v. S.F. Bay Area Rapid Transit Dist.*, No. 17-cv-02911-JSC, 2017 WL 6387764, at *5 (N.D. Cal. Dec. 14, 2017) ("A common meaning of 'device' is 'a

[2] Plaintiff focuses here on whether software or code qualifies as a device but also alleges that the software application worked in conjunction with "Defendant's servers in California"—indisputably "tangible" objects—to "eavesdrop on" the text messages at issue. *See* Compl. ¶¶ 109, 118.

thing made or adapted for a particular purpose… .'"; "Merriam-Webster defines 'device' in relevant part as 'a piece of equipment or a *mechanism* designed to serve a special purpose or perform a special function. . . .'" (emphasis added)). Nothing about "thing" or "mechanism" excludes software.

To the contrary, courts have explicitly held that "mechanism" *can* encompass software. *See, e.g.*, *United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wisc. 2019) ("The Court also agrees with the government's position that . . . 'mechanism' . . . seems to encompass software.") (citing *Merriam-Webster Dictionary*). The *Hutchins* court is not alone. "The majority of courts to consider this issue have entertained the notion that software may be considered a device for the purposes of the Wiretap Act." *Hutchins*, 361 F. Supp. 3d at 795 (citing, among other cases, *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1084–87 (N.D. Cal. 2015); *Luis v. Zang*, 833 F.3d 619, 630 (6th Cir. 2016) (software can be a device); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661–62 (E.D. Ten. 2012) (same)).

While it is true that the *Hutchins* court was interpreting the Wiretap Act and not CIPA, courts interpreting CIPA have looked to interpretations of the Wiretap Act for guidance when the Wiretap Act and CIPA use similar terms. *See, e.g.*, *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 606–07 (9th Cir. 2020) (looking to the Wiretap Act for guidance in evaluating claims under CIPA); *Licea v. Am. Eagle Outfitters, Inc.*, __ F. Supp. 3d __, 2023 WL 2469630, *8 (C.D. Cal. Mar. 7, 2023) ("Because the federal Wiretap Act also requires messages be intercepted while in

transit, courts have looked at cases analyzing the Wiretap Act as informative for CIPA."); *NovelPoster v. Javitch Canfield Group*, 140 F. Supp. 3d 938, 954 (N.D. Cal. 2014) ("The analysis for a violation of CIPA is the same as that under the federal Wiretap Act.").

The analogous portion of the Wiretap Act prohibits certain wiretapping activity involving an "electronic, mechanical, or other device." 18 U.S.C. § 2510(5). Though that phrase technically differs from the phrase "electronic amplifying or recording device" found in CIPA, the word "device" is what is at issue. There is nothing about the preceding modifiers ("electronic, mechanical, or other" in the Wiretap Act versus "electronic amplifying or recording" in CIPA) that would justify the "majority of courts" finding that software is included as a device in the former but not the latter.

The only case Defendant cites in support of its position involves a different provision of CIPA limited to an "electronic tracking device," which is defined as a device "attached to a vehicle or other moveable thing." *See In re Google Location History Litig.*, 428 F. Supp. 3d 185, 192–93 (N.D. Cal. 2019) (interpreting Cal. Penal Code § 637.7). There, the court focused on the word "attached" and found that software cannot be "attached" to something else. *See id.* at 194–96 ("Plaintiffs arguments that Defendants 'attached' an 'electronic tracking device' to a 'moveable thing' are rejected."). There is no similar "attached" requirement in Section 632.

///

///

B. Text messages can be confidential communications.

Under Section 632, "Confidential communication" is defined as

> any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication … the parties… may reasonably expect that the communication may be overheard or recorded.

Cal. Penal Code § 632(c). Whether a communication is confidential is an objective inquiry. That is, "[a] communication is 'confidential' under this definition if a party to the conversation had an *objectively reasonable expectation* that the conversation was *not being overheard or recorded*." *Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377, 1396 (2012) (emphases in original). "The issue whether there exists a reasonable expectation that no one is secretly recording or listening to a phone conversation is generally a question of fact." *Id.* at 1396. Significantly, a communication can still be confidential *even if the plaintiff should know it will later be disclosed*. *See id.* at 1397 ("[Arguments that a communication would be disseminated] reflect a misunderstanding of the applicable legal standard. The fact that plaintiffs may have known the information discussed in their phone calls would be disclosed . . . does not mean plaintiffs had no reasonable expectations that their telephone conversations were not being *secretly overheard*.") (emphasis in original). "'[C]onfidentiality' appears to require nothing more than the existence of a reasonable expectation by one of the parties that no one is 'listening in' or overhearing the conversation." *Frio v. Super. Court*, 203 Cal. App. 3d 1480, 1490 (1988).

The California Supreme Court has expressly adopted the *Frio* court's broad interpretation of confidentiality. *See Flanagan v. Flanagan*, 27 Cal.4th 766, 768 (2002). There, the court considered competing interpretations of when a communication is confidential: the first, that a conversation is confidential only if a party has an objectively reasonable expectation that its content will not be disseminated to others (which is the interpretation Defendant puts forth here); the second (the *Frio* interpretation), that a conversation is confidential if a party has an objectively reasonable expectation that the conversation is not being overheard or recorded simultaneously. *Id.* at 768. The court wrote that "[w]hile one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or a mechanical device." *Id.* at 775. The court then adopted the *Frio* standard, holding that "[b]y focusing on 'simultaneous dissemination,' not 'secondhand repetition', the *Frio* definition of 'confidential communication' . . . better fulfills the legislative purpose of the Privacy Act by giving greater protection to privacy interests . . . ." *Id.*

The California Supreme Court recently reiterated this holding. *See Smith*, 11 Cal.5th at 193, 200 (criticizing the Court of Appeals for its failure to examine *Flanagan* and reiterating the *Flanagan* holding: "secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and

extent of the firsthand dissemination of his statements" (internal quotation marks and citation omitted)); *see also Safari Club Int'l v. Rudolph*, 845 F.3d 1250, 1261 (9th Cir. 2017) ("The California Supreme Court found a conversation is confidential under section 632 if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded.") (internal quotation and citation omitted).

Despite these clear and binding holdings, Defendant's argument that a text message cannot be confidential rests entirely on the position that text messages are, by their nature, recorded on the recipient's device and by the telecommunications carrier, and can easily be forwarded or distributed. Mot. at 8–9. Not only does *Flanagan* foreclose Defendant's limited interpretation of confidentiality, but Plaintiff's claims do not rely on some illicit recording and subsequent distribution. Instead, Plaintiff's allegations here are that Defendant, without consent, eavesdropped upon the content of those messages before (and without ever) delivering them, and that Defendant further claims the right to refuse to deliver those messages if it does not approve of the content. *See* Compl. ¶¶ 30–38, 53, 66–67, 72–73. While Plaintiff may have arguably expected her text message would be *recorded* on LL Cool J's device, she did not and could not have expected it would be eavesdropped upon by Defendant, as alleged in the Complaint.[3]

[3] This is also one of myriad ways Defendant is not a telecommunications carrier, no matter how many times it tries to cloak itself in that mantle. Telecommunications carriers are passive and temporary storage intermediaries. They are not reading or

While it is true that there are cases finding that internet communications—such as email or online chat—are not confidential, those cases focused on claims of unlawful recording and subsequent dissemination, not unlawful *eavesdropping*. For example, Defendant relies heavily upon *In re Google Inc. Gmail Litig.*, 2013 WL 5366963 (N.D. Cal. Sept. 25, 2013). There, the court found confidentiality could not apply to emails based on a line of cases finding that "individuals cannot have a reasonable expectation that their online communications will not be recorded." *Id.* at *82–*83. True as that may be, this case is not about unlawful recording in and of itself, but unlawful eavesdropping. This distinction is clear from the cases upon which *In re Google* relies (some of which Defendant cites directly), which all deal with motions to suppress chat transcripts (i.e. recordings) introduced in criminal trials. *See People v. Nakai*, 183 Cal. App. 4th 499 (Cal. Ct. App. 2010) (denying motion to suppress explicit Yahoo! Chat transcript between adult and individual posing as minor); *People v. Cho*, 2010 WL 4380113 (Cal. Ct. App. Nov. 5, 2010) (unpublished) (same); *People v. Griffitt*, 2010 WL 5006815 (Cal. Ct. App. Dec. 9, 2010) (unpublished) (same).[4] *Campbell v. Facebook* relied on these same, inapposite cases. 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014).

///

analyzing text messages and refusing to deliver those messages if the messages do not meet some arbitrary, content-based test, or if the sender refuses to sign up for service with that carrier.

[4] Notably, *none* of these cases addressed—or even mentioned—*Flanagan*, presumably because only recording (rather than simultaneous dissemination) was at issue.

This distinction between *eavesdropping* and *recording*—and those being separate paths to liability—is the easiest way to reconcile any tension between *Flanagan* and *In re Google*. In other words, it is possible that both Plaintiff and Defendant are correct generally, but Defendant's arguments relate to a case not before the Court. It may be true, as Defendant argues, that a plaintiff cannot have an objectively reasonable expectation of privacy that a written, electronic communication would not be recorded, thereby foreclosing any Section 632 claim based on the simple act of recording those communications.[5] It may also be true, however, that a plaintiff *can* have an objectively reasonable expectation of privacy that a written, electronic communication is not being eavesdropped upon by "an unannounced second auditor, whether that auditor be a person or a mechanical device." *Flanagan*, 27 Cal. 4th at 775. This case concerns the latter.

Nevertheless, even if the Court is inclined to adopt a general presumption that written communications are not typically confidential, this presumption is rebuttable. *See Revitch, LLC,* 2019 WL 5485330, at *3 (analyzing the circumstances of internet communications and declining to deviate from the "general rule"); *Rodriguez v. Google, LLC,* 2021 U.S. Dist. LEXIS 98074, at *7 (N.D. Cal. May 21, 2021) (any presumption against online confidentiality is rebuttable). Whether the circumstances here warrant departure from this presumption is a question of fact. Defendant's entire

[5] This is intended to refer only to a Section 632 claim, not Section 632.7, under which liability *may* lie for the simple act of receiving and recording by any entity without the consent of all Parties.

business is built on creating an objectively reasonable expectation of privacy in the text messages with its Community Leaders, or, as it writes on its site, giving the appearance of "texting artists, celebrities, visionaries—the leaders you respect and admire—the same way you do with your mom or best friend." *Introducing Community*, https://www.community.com/post/introducing-community (last visited July 24, 2023). As Defendant also states on its site, "[o]ur phone numbers are precious and personal. Giving out your phone number feels like an intimate exchange," and that its goal is to create "real, meaningful connection . . . [b]etween artists and fans, creators and patrons, faith leaders and congregants, companies and customers, elected officials and constituents." *Id.* Defendant cannot now claim that it was unreasonable for Plaintiff to believe the illusion Defendant clearly set out to create and upon which its entire business model is based.

III. Plaintiff States a Valid Claim for Violation of Section 632.7

A. Plaintiff is not required to allege the use of two phones.

Defendant argues that Plaintiff must allege that there were two phones involved in the subject communications. Defendant is incorrect.

To state a claim for violation of Section 632.7, Plaintiff need only allege that at least one cell phone or cordless phone was used in the subject communication, and she alleges that she used her cell phone to send the subject text message. *See* Compl. ¶ 62. In *McCabe v. Six Continents Hotels, Inc.*, the court denied a motion to dismiss a Section 632.7 claim in part because the plaintiffs "are not required to allege the type

of device [the defendant] used to receive [the] calls" at issue. 2014 WL 465750, at *4 (N.D. Cal. Feb. 3, 2014). There, the court described other courts' characterization of "the statute as prohibiting 'the intentional recording of any communication without the consent of all parties where *one of* the parties is using a cellular or cordless telephone.'" *Id.* at *3 (emphasis added) (*quoting Zephyr v. Saxon Mortg. Services, Inc.*, 873 F. Supp. 1223, 1225 (E.D. Cal. 2012)); *accord Roberts v. Wyndham Int'l, Inc.*, No. 12-cv-5180 PSG, 2012 WL 6001459, at *4 (N.D. Cal. Nov. 30, 2012); *Kuschner v. Nationwide Credit, Inc.*, 256 F.R.D. 684, 688 (E.D. Cal. 2009).

"This interpretation comports with the California Supreme Court's discussion of § 632.7 in *Flanagan v. Flanagan*, in which the Supreme Court stated that § 632.7 prohibited the 'intentional interception or recording of a communication involving *a* cellular phone or *a* cordless phone.'" *McCabe*, 2014 WL 465750, at *6 (emphasis added) (quoting 27 Cal.4th 766, 776 (2002)). In *Flanagan*, the California Supreme Court stated that CIPA "protects against the intentional, nonconsensual recording of telephone conversations regardless of the content of the conversation or the type of telephone involved." 27 Cal.4th at 776. The *McCabe* court further noted that the legislative analysis of CIPA describes Section 632.7 as making punishable "the interception and intentional recording of a communication transmitted between two telephones, *one or both of which is a cellular, cordless or landline* telephone without the consent of all parties to that communication." *McCabe*, 2014 WL 465750, at *7 (emphasis added) (internal quotation and citation omitted).

In addition, Section 632.7 has been applied to "internet-based communications and written communications." *Licea v. Old Navy, LLC*, No. 5:22-cv-01413-SSS-SPx, 2023 WL 3012527, at *10 (C.D. Cal. Apr. 19, 2023). In *Brown v. Google, LLC*, for example, the court concluded that internet-based communications fall within the scope of Section 632.7 where there is a reasonable expectation of privacy in the communications. 525 F. Supp. 3d 1049, 1073–74 (N.D. Ca. 2021). "[A] conversation is confidential under section 632 if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan*, 27 Cal.4th at 776. Here, Defendant overheard and recorded Plaintiff's text to LL Cool J when it intercepted that text message, did not deliver it to LL Cool J, and stored that text message, recording its contents in its own records while Plaintiff had no idea that the message would be so intercepted.[6] *See* Compl. ¶¶ 33, 35, 38, 62. Prior to sending the text message, Plaintiff reasonably expected that it would not be intercepted and/or recorded by Defendant before it ever reached LL Cool J. *Id.* ¶¶ 34, 45. Thus, Plaintiff's text message was confidential when she sent it from her cell phone.

Plaintiff adequately pleads her claim for violation of Section 632.7 because she

[6] This Court has previously declined "to definitively resolve whether Plaintiffs could not possess a reasonable expectation that no one was secretly recording their messages, . . . particularly when Defendant operates a platform intended to build a more personal connection than possible on social platforms or via email." *Adler v. Community.com, Inc.*, 2021 WL 4805435, at *5 (C.D. Cal. Aug. 2, 2021) (internal quotations omitted).

had an objectively reasonable expectation of confidentiality in her text to LL Cool J and alleges the use of at least one cell phone in sending that text message.

B. Plaintiff alleges the use of two cell phones.

Even if the Court requires that Plaintiff plead the involvement of two devices, she has done so. Plaintiff alleges that she sent her text message from her cell phone to LL Cool J's cell phone. *See* Compl. ¶ 16–17, 45–46, 56, 62–63, 77. Defendant's interception of that text, however, prevented the text from ever reaching LL Cool J's cell phone.

Nevertheless, it cannot be that a third party who takes a message in transit from one cell phone to another is not liable because, by virtue of their theft, the message never reached the second, "qualifying" device. The only logical reading of Section 632.7 requires analyzing the expected pathway of the communication when sent. Here, the text communication was supposed to go from cell phone to cell phone (as any other text message). Furthermore, the nature of the devices involved in the communication at issue is a fact question that cannot be resolved with Defendant's motion. For example, if LL Cool J accessed his Community messages through an app on his cell phone, then the communication was transmitted between two cell phones.

C. Plaintiff alleges Defendant intercepted her text communication.

Defendant claims that Plaintiff does not state a claim under Section 632.7 "for failure to allege Community 'intercepts' messages." Mot. at 12. As discussed

more below, Section 632.7 is not confined to interceptions; it also prohibits "receiv[ing] and intentionally record[ing]" electronic communications without consent. *Smith*, 11 Cal.5th at 193. Still, focusing exclusively on the interception alternative, Defendant's argument is incorrect.

First, as pled, when anyone, including Plaintiff, first texts a Community Leader at their Community number, Defendant "intercepts and records, without consent, the initial messages intended for its celebrity clients and essentially holds them hostage from the celebrity clients until the sender signs up for Defendant's social networking service." Compl. ¶ 35.

Second, since the Court last addressed this question in *Adler*, Defendant has doubled down on its harmful practices. Defendant's policies now outright state that Defendant intercepts initial text messages intended for its Community Leaders, holding them unless and until a texting consumer signs up for its services and Defendant has deemed the message content acceptable. Specifically, Defendant's privacy policy now states that it "may access, review, block (including limiting Community Leaders' ability to access messages), or delete your messages at any time and for any reason." Compl. ¶ 33. Thus, unbeknownst to Plaintiff, Defendant can, and does, "block" messages from arriving at the Community Leader number. That blocking is an interception under even the strictest and most narrow interpretation of an "intercept" for the purposes of Section 632.7. *See Konop*, 302 F.3d at 878. Indeed, as this Court wrote in *Adler*, "Plaintiffs do not seem to dispute

that Defendant could not access the contents of the text messages at issue until they were received at the celebrity's Community number." 2021 WL 4805435, at *3. In light of Defendant's disclosures in its privacy policy, however, Plaintiff Boulton pleads just that. Defendant unlawfully accesses, eavesdrops upon, and reviews messages intended for Community Leaders *before* they ever reach those numbers and completes delivery only after the sender signs up *and* Defendant deems the content of the message acceptable.

Accordingly, Plaintiff states a claim under Section 632.7 based on Defendant's interception of her text message to LL Cool J.

D. Defendant is also liable under Section 632.7 because it received and recorded Plaintiff's text communication without her consent.

Defendant is liable to Plaintiff under Section 632.7 due to its receipt and recording of Plaintiff's text message to LL Cool J, regardless of whether that text message was intercepted in transit. Section 632.7 provides that punishment shall issue to "[e]very person who, without the consent of all of the parties to a communication, intercepts *or receives and intentionally records*, or assists in the interception or reception and intentional recordation of, a [telephone] communication." Cal. Penal Code § 632.7(a) (emphasis added). Section 632.7 is expressly made applicable to all communications, written or otherwise. Cal. Penal Code § 632.7(d)(3) (defining "communication" to include, among other things,

communications transmitted by "data, or image, including facsimile"). Section 632.7 does *not* contain a "confidential" requirement.

Defendant's privacy policies state that it collects the text messages, "including message-related information (such as the phone number from which the message was sent, when the message was sent, [and] the content of the message . . .)." Compl. ¶¶ 29–30. Plaintiff did not, and could not have, consented to these policies of taking of her text communication to LL Cool J since "these policies are not disclosed to consumers (like Plaintiff[]) prior to their initial text to one of Defendant's Community Leaders." *Id.* ¶ 34; *see also id.* ¶ 54 ("At no point prior to sending the initial text message [was Plaintiff] informed of, nor did [she] consent to, Defendant's collection and scanning of the text message intended for [the] celebrity."). "In other words, Defendant intercepts and records, without consent, the initial messages intended for its celebrity clients and essentially holds them hostage from the celebrity clients until the sender signs up for Defendant's social networking service." *Id.* ¶ 35.

Plaintiff states a claim under Section 632.7 based on Defendant's receipt and recording of her text message to LL Cool J.

CONCLUSION

Having failed to dismiss these same claims in *Adler*, Defendant's arguments here fare no better. The Court should deny the motion to dismiss so that the parties may begin discovery.

Dated: July 26, 2023

LIPPSMITH LLP

By: /s/ *Graham B. LippSmith*
GRAHAM B. LIPPSMITH
MARYBETH LIPPSMITH
JACLYN L. ANDERSON

TOUSLEY BRAIN STEPHENS PLLC
JASON T. DENNETT
KALEIGH N. BOYD

GLAPION LAW FIRM, LLC
JEREMY M. GLAPION

Attorneys for Plaintiffs